Computer
& Robotics

A Secure Channel to Improve Energy Cost in Internet of Things

Kobra Karkhaneh, Mohammad Mehdi Gilanian Sadeghi*

Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Received 26 March 2018; Revised 17 January 2019; Accepted 18 February 2020; Available online 11 May 2020

Abstract

The sensors in the Internet of things, especially in the health sector, requires a secure platform for data transfer. Because of the widespread use of the Internet of things, the security and longevity of these networks are becoming increasingly important. In this paper, we propose a secure channel between the group of sensors, server, and third party, as well as saving energy consumption of sensors. This channel contains a series of information, including exchanged messages between group members, servers, and a third-party that is used to perform secure encryption and authentication operations, so that sensors are safely assigned to the server and transfer the data securely. The results show that the proposed method has less communication and computational costs. Also, the energy consumption of the sensors in the channel is reduced by up to 40%.

Keywords: *Internet of things, key management, secure channel, energy.*

1. Introduction

With the advancement of technology, our community moves forward to communicate with each other and everyone. The Internet of things (IoT) establishes a connection for each person and anything at any time and place. The number of Internet-connected devices is rising at a fast rate. At first, the Internet of things concept used by Kevin Ashton in 1999 [1]. He describes a world in which everything has a digital identity and allows computers to organize and manage them. The IoT faces security and confidentiality challenges because it has expanded the Internet from the traditional Internet, and with this kind of Internet, anything can be connected, and things can be interconnected. Here, the things make groups; and then members of each group should share their data in a secure environment, so one of the basic needs is to provide a secure and reliable platform for objects in sensors of the IoT [2].

On the other hand, due to the vast applications of the IoT for various uses, the communication and computational costs along with the energy consumption of these networks, are important. Due to the limited energy of the sensors in the IoT, the communication and computational costs and energy consumption of the sensors should be decreased. Therefore, providing a reliable communication channel requires more optimal energy. In this paper, we intend to propose a secure environment between group members and servers to ensure that the group members are safe from threats and can share their information and key with the server. We also have a third party that reduces energy

* Corresponding author. Email: msadeghi@ieee.org

consumption in sensors. In fact, messages are distributed between sensors, servers, and the third party, so that the costs of the computational and communication of the sensors are reduced [3].

The paper is structured as follows. We first describe the related works in Section II. In Section III, the proposed method is explained, and then in Section IV, the performance of the method is analyzed. Finally, in Section V, the simulation and comparison results are presented.

2. Related Works

Many recent works have investigated the usability of cryptographic algorithms in the context of wireless sensor networks. For instance, symmetric encryption using AES is discussed in [4] and [5]. For public-key cryptography, the implementation of Elliptic Curve Cryptography (ECC [6]) on sensors is described in [7] and [8]. Several previous works have focused on the energy cost of key agreement protocols for wireless sensor networks. Based on the first implementation of ECC and RSA on 8-bit microprocessors by [9] and [10] quantified the energy costs of ECC and RSA based digital signature and key exchange with mutual authentication for networks composed of Mica2Dot sensors. They concluded that these operations are affordable for such sensors. The authors in [11] compared the cost of the Kerberos and ECDH protocols on 32-bit WINS sensor nodes. The cost of Diffie-Hellman was found between one to two orders of magnitude larger than AES-based Kerberos. The authors in [12] performed the same comparison but with another version of Diffie- Hellman, ECMQV, on WINS nodes. They found that the cost of ECMQV was only up to twice the cost of Kerberos [13,14].

Abdmeziem and Tandjaoui considered four components in the network model (SKME) [15]:

1. Mobile and contextual sensors: the sensors are planted in, on or around a human body to collect health-related data (e.g. blood pressure, blood glucose level, temperature level, etc.).

2. Third parties: the third parties represent a key component in the protocol. A third party could be any entity able to perform high consuming computations on behalf of the sensor nodes. In fact, the resource-constrained sensors rely on them by offloading high consuming cryptographic primitives in a cooperative way.

3. Remote server: the remote server receives the gathered data for further processing. A remote server could be used by caregiver services in order to take appropriate decisions according to the patient's data.

4. Certification authority: the certification authority is required to guarantee authentication between the third parties and the remote server by delivering authenticated certificates.

In SKME's approach, initially, the sensors should establish a shared secret to a remote server. So each sensor generates a secret key called S, which divides randomly it into several parts S_1, S_2… S_n in turn and the number of shared keys is proportional to the number of third parties. In the next step, each sensor encrypts these secret parts and sends them to each corresponding third party. Encryption at this stage is based on symmetric cryptography using the pre-shared key.

Additionally, MAC (Message Authentication Code) messages are used for authentication. Each third party receives its corresponding secret part and delivers it to the remote server, which is an asymmetric encryption step that utilizes the public key of the remote server. The remote server receives these secret parts and decodes them, and combines the secret parts into the secrets that the sensor sent [15-17]. Fig.1 illustrates the SKME network model, and Table 1 contains the notations used in this paper.

Table 1: Notations [15]

Notation	Description
A	Sensor
TP	Third party
S	Server
N	Nonce number of sensor
R	Random number generated by node
N	Number of group
P	Prime number of Z_p
K	Key
K_G	Group key
K_K	Public key of node x
$K_{x,y}$	Key between x and y
Sign	Digital signature

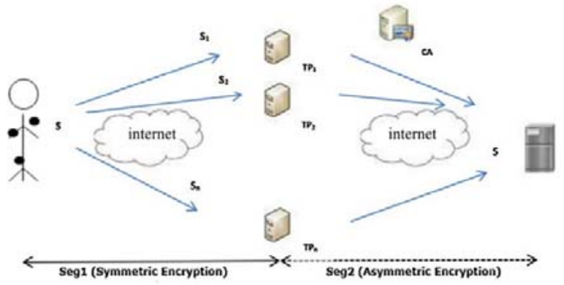

Fig. 1. SKME network model [15].

3. Proposed Method

There are several nodes or sensors that want to be members of the group in the network. We use the Poisson distribution with a specific arrival rate for membership. After entering the members, the service is provided to the service group, which includes a series of transmitted information between the sensors and the third party and the server. This information is messages for establishing a secure connection. Encryption and authentication are used to secure these messages. In fact, these transmitted messages are used to introduce group members to the server and the third party, and vice versa. The result is to create a two-way channel between these entities so that the server can generate the key of the group with the members. This service is provided to members of the group with a fixed rate with an exponential distribution. After collecting the necessary information for the server, the server generates the group key. The group members need a group key to transmit their information securely. Therefore, it is essential to secure the group key for this secure channel creation method.

The steps to create a secure channel are through messages that are used to assign the group members to the server and exchange the necessary information between them, which uses a third party to reduce node overhead. For each member of the group, there is a third party of its own, in which the necessary information is exchanged between the two. The information is sent between the member and the server through this third party. The sensors (members) have their own public keys that encrypt and send messages by this key. The third-party also has a public key as well as a shared key with the sensors that some of the messages between them are encrypted by these two keys. Therefore, sensor activities would be less, and then less energy would be consumed. That is the advantage of the proposed method in which we assign all the numbers from the group of integers on the basis of the prime number p, where p is a large number.

The proposed method makes a secure channel for exchanging information between the server and the sensors. The result of this is to prevent eavesdropping and attack on information exchanged between them. To do this, the group sensors need to send their random numbers securely through this secure channel to the server so that the server can generate the group key group with the help of these random numbers. This channel is secured through the messages shown in Fig.2.

Message 1: The group's initiator, which is a member of the group, sends a message called "Hello" that includes the number of group members, the random number of each member (sensor), and security policies, such as the encryption method and the key in order to encrypt the information, to the server as $Hello[n\ |p\ |N_i\ |security\ policy]$. But other members of the message group only send a random number and security policies.

Message 2: After receiving the first message, the server returns to the initiator, a message called Hello, which contains the random number of the sensor and the random number of the server and the security policy agreement.

Message 3: In the third message, it is assumed to be a common key between the third party and the sensor. In this message, the sensor needs to inform the third party of the random number of itself and the server, which is encrypted with the key between the sensor and the third party, $K_{Ai,TP}$.

Message 4: The third party sends the acknowledgment message to the sensor via the MAC and sends all the received information and its random number to the sensor.

Message 5: The third party sends its certificate to the server, and also requests the server certificate. In this message, he sends his random number and the server for further emphasis.

Message 6: The server sends its certificate for the third party. Note that all messages contain nonce to prevent repeat attacks.

Message 7: In this message, the server requests the key between the sensor and the third party from the sensor.

Message 8: The sensor uses a hash function for the key between itself and the third party and then sends it to the server.

Message 9: The sensor applies the pseudo-random function on the random number of the third party and its random number, and gets a random number $r_i=f(N_{TP}\ |N_i)$. The sensor then adds its random number and the random number of the server to the prime number $p \in z_p$ and calculates the number w_i, *so that* $r_i+r_s=w_i \bmod p$. After these two operations, the sensor encrypts the random number with the key between itself and the third party and sends it to the third party.

Message 10: The random number of the sensor, the server, and the hash function of the key between the sensor and the third party are signed by which encrypts all the messages with the public key of the server and sends it to the server.

4. Performance Analysis

In the previous section, we proposed a secure channel for exchanging information between the sensors of a group and a server. In this section, the parameters of the computational cost, communication cost, and the energy consumption for group sensors would evaluate. The operation of sending and receiving data by each sensor node in the Internet of things is one of the operations that would drain the energy of the sensor nodes. If these operations reduced, the lifetime of the sensor nodes would become longer. The total cost of communication for group sensors is the total cost of sending and receiving messages. In the cryptographic discussion for the channel, there is a need for a key between the sensor, the third party, and the server. Also, they must be authenticated in the model. In fact, the total cost of encryption and authentication would consider as computational cost. The next parameter is the energy consumption of sensor nodes, which is one of the most important parameters in the Internet of things, and that is considered for the design of the protocols Internet of things [15].

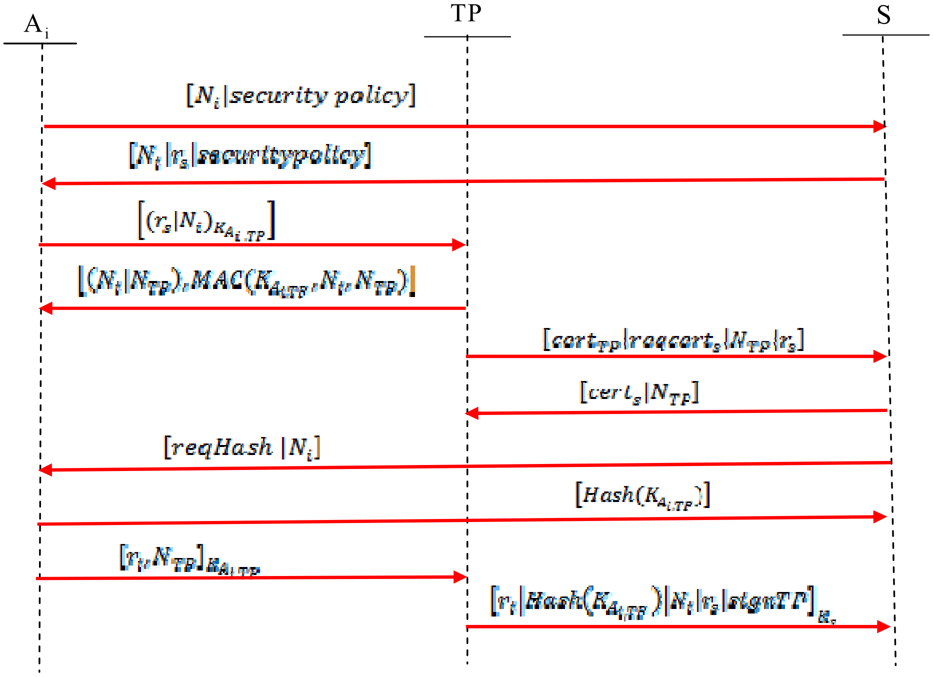
A_i
TP
S
$[N_i|security\ policy]$
$[N_i|r_s|securitypolicy]$
$[(r_s|N_i)_{K_{A_i,TP}}]$
$[(N_i|N_{TP}), MAC(K_{A_i,TP}, N_i, N_{TP})]$
$[cert_{TP}|reqcert_s|N_{TP}|r_s]$
$[cert_s|N_{TP}]$
$[reqHash\ |N_i]$
$[Hash(K_{A_i,TP})]$
$[r_i, N_{TP}]_{K_{A_i,TP}}$
$[r_i|Hash(K_{A_i,TP})|N_i|r_s|signTP]_{K_s}$

Fig. 2. Messages in the channel.

4.1. Communication Cost

To calculate the communication cost, the messages that are exchanged in this model would consider. In this case, messages that group members send, and messages sent from the third party and the server to the group sensors are considered to calculate the communication cost of the sensors which is written below.

- Sending Cost: The cost of sending messages by the sensors.
- Receiving Cost: The cost of receiving messages by the sensors.

Therefore, the communication costs are expressed as follows:

(Communication =Sending + Receiving) cost (1)

To calculate this relationship, we need the size of the messages exchanged by the sensors of the group, which we use from Table 2 [15].

Table 2: Size of messages exchanged by group sensors [15]

Exchanged message	Size (bytes)
Message1	104
Message2	104
Message3	88
Message4	64
Message7	14
Message8	20
Message9	100

Now we can see the cost of sending and receiving in Table 3.

Table 3: Cost of sending and receiving for each sensor

Type message	Messages	Size (bytes)
Sending messages	1،3،8،9	312
Receiving messages	2،4،7	182

By calculating the cost of sending and receiving, we can calculate the communication cost from the sum of these two factors, which results in 494 bytes.

4.2. Computational Cost

The cost used to calculate encryption and authentication operations is considered for the computational cost. In other words, the relation of computational cost is as follows:

(Computational = Encryption +Authentication) Cost (2)

We use the AES-128-bit (16-byte) symmetric encryption method to encrypt messages, and we use the MAC Authentication Code for the 128-bit SHA-1 to authenticate. To do this, we consider which messages use for encryption and authentication, then, according to Table 2, the messages are calculated. The cost of authentication and encryption operation is shown in Table 4.

Table 4: Cost of encryption and authentication

Type message	Messages	Size (bytes)
Encryption messages	9،3	188
Authentication messages	4	64

By calculating these two factors, the computational cost is 252 bytes.

4.3. Total Energy Cost

One of the aims of the proposed method is to reduce energy consumption. Therefore, we need a standardized model for calculating the energy consumption in the Internet of things network. In this model, considering that the energy needed to transmit data packets between sensor nodes is more important than other network energy consumed. The major part of the energy consumption of the network is related to the reception or transmission of data. Therefore, the relationship between the energy consumption models is as follows:

(Energy =Communication +Computational) Cost (3)

To calculate the cost of send and receive energy consumption, we need to Table 5, which expresses the desired size in terms of micro-joule.

Table 5: Transmission energy in a sensor

Operation	Energy consumption (μJ)
transmit 1 bit	0.72
Receive 1 bit	0.81

Now, with the help of Table 5, we can calculate the amount of energy used to send and receive messages, as shown in Table 6.

Table 6: Transmission energy in a sensor

Type message	Messages	Size (bytes)	Energy consumption (µJ)
Sending messages	1،3،8،9	312	1797.12
Receiving messages	2،4،7	182	1179.36

With a total of two sending and receiving costs in the sensor, we can get the amount of energy consumed by communications up to 2976.48 micro-jules.

Table 7: Computational cost in a sensor

Operation	Energy consumption (µJ)
Encryption AES-128	28.11
MAC-128	23.9

According to Table 7, the computational cost is expressed in a sensor, namely, encryption and authentication operations. Now, with the help of Table 7, we can calculate the amount of energy used for encryption and authentication, and the result is shown in Table 8.

Table 8: Cost of encryption and authentication

Type message	Messages	Size (bytes)	Energy consumption (µJ)
Encryption messages	9،3	188	330.2925
Authentication messages	4	64	95.6

By calculating these two factors, we can calculate the computational cost in micro-joule, which is equal to 425.8925 micro-jules. The result of the total energy consumption is shown in Table 9.

Table 9: Total energy cost

Communication cost	Computational cost	Total energy cost
2976.48	425.8925	3402.3725

5. Simulation

In the proposed method called SCECIOT , there are several sensor nodes that want to join a group. Here, for membership we use Poisson distribution with a specified entry rate. After the nodes entered the group, they are provided a set of information that is transmitted between these sensors and the third party and the server, including messages to establish a secure connection. Encryption and authentication operations are used to safely transmit these messages. In fact, the exchange of messages to identify group members to the server and the third party, and vice versa, creates a two-way channel between these entities so that the server can generate the group key with known member information. For example, suppose n members A1, A2, …, An are randomly assigned to the group over the period of time [t1,tm]. These members enter the group at different times and at random times as shown in Fig. 3.

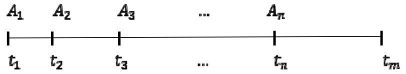

Fig. 3. Allocate time to group members

In this scenario, suppose 60 sensors in one day, [0,1440] minutes, want to go into the IoT, and get service. The pseudo-code for executing this scenario is shown in Fig. 4 which is simulated by Matlab software.

```
Set value of the group size n
For (i=1:i≤ n) do
Evaluate Poisson distribution for each member of group(T(i));
End
For (i=1:i≤ n) do
If  T(i)<T(i+1)
Calculate service value for each member of group according table VII , VIII (m(i));
else
Increase one  unit to counter
end
For (j=1:i≤ n) do
evaluate SCECIOT Communication energy in the table IX (er(j));
evaluate SKME Communication energy (eerr(j));
end
For (j=1:i≤ n) do
calculate SCECIOT Computational energy in the table IX (mo(j)) ;
calculate SKME Computational energy (mmoo(j));
end
For (j=1:i≤ n) do
totalenergy(j)=SCECIOT Communication energy+ SCECIOT Computational energy;
totalenergy(j)=SKME Communication energy +SKME Computational energy ;
end
```

Fig. 4. The proposed SCECIOT

In this section, we compare the energy consumption of the SKME method [15] with the proposed SCECIOT method and then estimate the percentage of energy reduction. Fig. 5 shows the amount of communication energy of the group members, and Fig. 6 compares the computational energy of the members. The cost of computing is usually less than the cost of communicating for sensors. Fig. 7 shows the total energy consumption, which is based on both communication and computational costs. Here, as it is observed in Fig. 7, when the time goes on, the total energy consumption increases. In the proposed method, the total energy consumption is reduced by about 40% compared to the SKME method. This amount of energy-saving plays an important role in the life of the sensors.

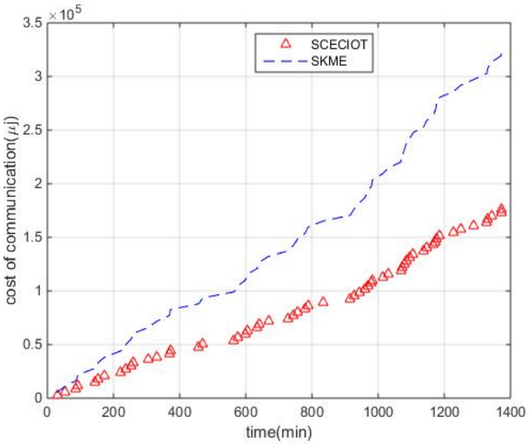

Fig. 5. Communication energy in the time interval

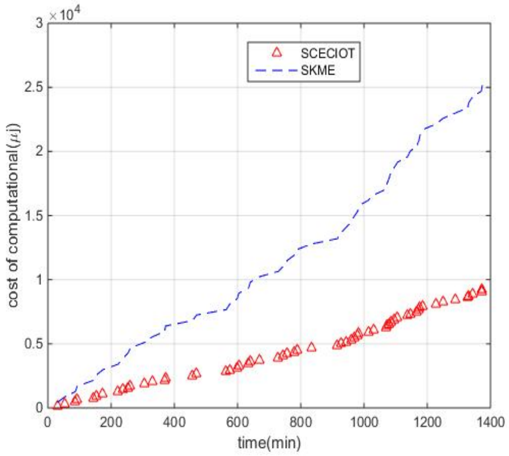

Fig. 6. Computational energy in a time interval

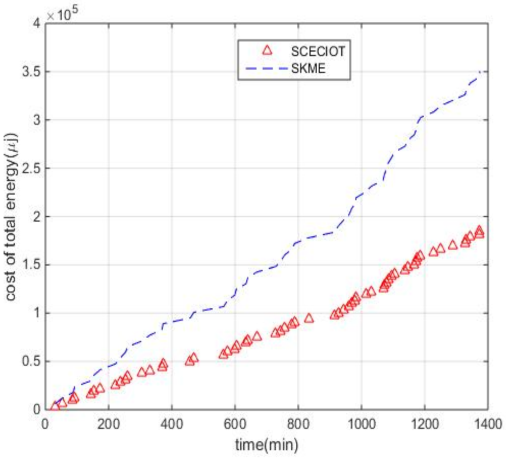

Fig. 7. Total energy cost of the sensor over time

6. Conclusion

The security of Internet things plays an important role in these networks. On the other hand, to reduce the energy consumption of sensors is important also. In this paper, a new method has been proposed to enhance the security of the network's entities. In this regard, a point-to-point secure channel between a group of members and server has created. In this secure channel, we use the third party to get the data to the server in order to reduce the operation of the sensor, and thus not reducing sensor lifespan. In the proposed method, we significantly reduced the amount of energy consumption of the sensors in the group.

7. Future Work

In this way, we used a third element channel to provide security. Generally, increasing the security of the IoT networks requires energy consumption and, in fact, there is a tradeoff between security and energy. In the future, with the provision of a secure channel, we are looking for a way to calculate the group key that is associated with less energy consumption in the sensors, so that the group members can communicate with the generated group key safely.

References

[1] Yan, Z.; Zhang, P., "A survey on trust management for Internet of Things", In Journal of Network and Computer Applications, vol. 42, no. 17, pp. 120-134(2014).

[2] Prabhu, M.; Seethalakshmi, G., "Secured hearth care system in IoT", In International Journal of Pure and Applied Mathematics, vol. 118, no. 20, pp. 3239-3244 (2018).

[3] Chen, X.Y.; Jin, Z.G., "Reseach on key technology and applications for Internet of things", In Physics Procedia, vol. 33, no. 12, pp. 561-566 (2012).

[4] Healy, M.; Newe, T., "Efficiently securing data on a wireless sensor network", In Journal of Physics Conference Series, IOP Publishing, vol. 76, no. 1, p. 012063 (2007).

[5] Law, Y.; Doumen, J., "Survey and benchmark of block ciphers for wireless sensor networks", In ACM Transactions on Sensor Networks (TOSN), vol. 2, no. 1, pp. 65–93 (2006).

[6] Hankerson, D.; Menezes, A., "Guide to elliptic curve cryptography", Springer scince & business Media (2003).

[7] Gupta, V.; Millard, M., "Sizzle: A standards-based end-to-end security architecture for the embedded Internet", In Pervasive and Mobile Computing, vol. 1, no. 4, pp. 425-445 (2005).

[8] Liu, A.; Ning, P., "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks", In International Conference on Information Processing in Sensor Networks, IEEE, pp. 245-256 (2008).

[9] Gura, N.; Patel, A., "Comparing elliptic curve cryptography and RSA on 8-bit CPUs", In International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, pp. 119-132 (2004).

[10] Piotrowski, K.; Langendoerfer, P., "How public key cryptography influences wireless sensor node lifetime", In Proceedings of the Fourth ACM Workshop on Security of ad hoc and sensor networks, ACM, NY, USA, pp. 169-176 (2006).

[11] Hodjat, A.; Verbauwhede, I., "The energy cost of secrets in ad-hoc networks", In Proceeding of IEEE Circuits and Systems Workshop on Wireless Communications and Networking (2002).

[12] Großschadl, J.; Szekely, A., "The energy cost of cryptographic key establishment in wireless sensor networks", In Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ACM, pp. 380-382 (2007).

[13] Wander, A.; Gura, N., "Energy analysis of public-key cryptography for wireless sensor networks", In Third IEEE International Conference on Pervasive Computing and Communications, pp. 324–328 (2005).

[14] Law, Y.; Doumen, J., "Survey and benchmark of block ciphers for wireless sensor networks", ACM Transactions on Sensor Networks, vol. 2, no. 1, pp. 65–93 (2016).

[15] Abdmeziem, M.; Tandjaoui, D., "An end-to-end secure key management protocol for e-health applications", Computers and Electrical Engineering, vol. 44, no. 7, pp. 184-197 (2015).

[16] Jianga, Qi.; Maa, J., "Efficient end-to-end authentication protocol for wearable health monitoring systems", Computers and Electrical Engineering, vol. 63, pp. 182-195 (2017).

[17] Prabhu, M.; Seethalakshmi, G., "Secured hearth care system in IoT", In International Journal of Pure and Applied Mathematics, vol. 118, no. 20, pp. 3239-3244 (2018).